Systême soft

Программный комплекс Систэм Платформ

SePlatform.HMI.SecurityConfigurator 2.2

Руководство пользователя

Редакция	Соответствует версии ПО
1. Предварительная	2.2.1

Содержание

1. Руководство пользователя

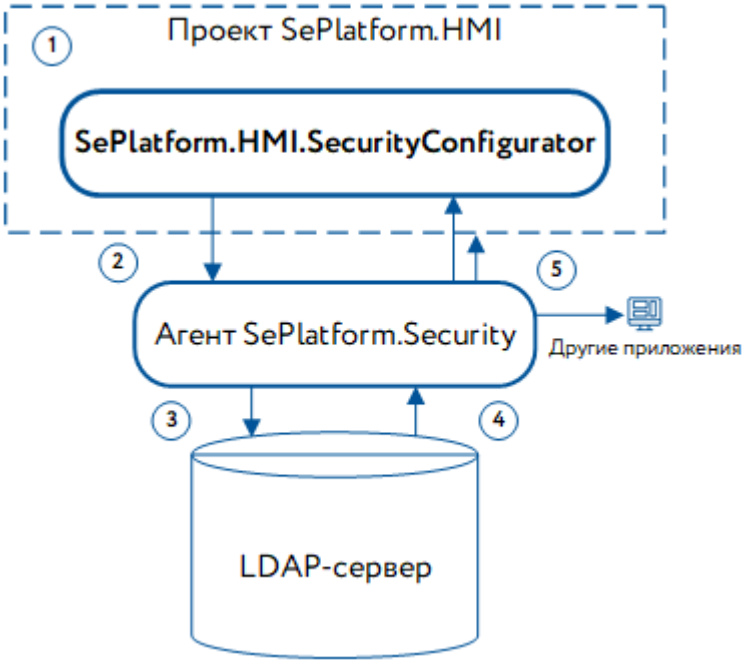
1.1. О продукте

SePlatform.HMI.SecurityConfigurator - приложение, предназначенное для конфигурирования подсистемы безопасности SePlatform.Security.

Под конфигурированием подсистемы безопасности подразумевается:

- создание учетных записей пользователей для предоставления им доступа к возможностям проекта;
- объединение пользователей в группы для предоставления им одинаковых возможностей;
- создание прав доступа к возможностям проекта и группировка прав в приложения;
- создание ролей и назначение их пользователям или группам;
- назначение прав пользователям, группам и/или ролям.

Используйте SePlatform.HMI.SecurityConfigurator как самостоятельное приложение, или встраивайте его в проекты автоматизации, разработанные в SePlatform.HMI. Подробнее в 1.3. Запуск приложения (стр. 7). Роль SePlatform.HMI.SecurityConfigurator в схеме взаимодействия с SePlatform.Security и другими приложениями можно описать следующей иллюстрацией:



1. SePlatform.HMI.SecurityConfigurator встраивается в проект автоматизации, реализованный в среде разработки SePlatform.HMI, или вызывается как самостоятельное приложение.
2. С помощью SePlatform.HMI.SecurityConfigurator меняется конфигурация подсистемы безопасности SePlatform.Security. Новая конфигурация передается Агент SePlatform.Security.
3. Агент SePlatform.Security записывает на LDAP-сервер конфигурацию, где она хранится в виде каталогов LDAP.
4. LDAP-сервер по запросу предоставляет информацию о пользователях, группах, ролях и их возможностях Агент SePlatform.Security.
5. Агент SePlatform.Security предоставляет информацию всем приложениям, запрашивающим ее.

1.2. Подготовка к работе

Требования к окружению

Для работы SePlatform.HMI.SecurityConfigurator должны быть установлены:

- SePlatform.HMI - среда разработки проектов автоматизации;
- SePlatform.Security - подсистема безопасности, которую можно конфигурировать в соответствии с нуждами проекта;
- SePlatform.Domain - компонент, обеспечивающий взаимодействие между SePlatform.HMI и SePlatform.Security;
- SePlatform.HMI.Security - компонент, обеспечивающее взаимодействие приложения с SePlatform.Security;
- SePlatform.HMI.Tables - компонент, обеспечивающий отображение компонентов приложения в проекте в режиме исполнения.

Если приложение используется в веб-версии проекта автоматизации, то установите дополнительно:

- SePlatform.HMI.WebViewer - для просмотра проектов SePlatform.HMI в веб-интерфейсе;
- SePlatform.HMI.Security.WebViewer - для работы компонентов SePlatform.HMI.Security в веб-интерфейсе;
- SePlatform.HMI.Tables.WebViewer - для работы компонентов SePlatform.HMI.Tables в веб-интерфейсе.

Если необходимо подключить SePlatform.HMI.SecurityConfigurator к проекту SePlatform.HMI, установите также SePlatform.HMI.CommonLib.

Установка, удаление или восстановление

ОС Windows

Для установки, удаления или восстановления SePlatform.HMI.SecurityConfigurator запустите установочный файл `seplatform.hmi.securityconfigurator-<lng>-<version>.<arch>.msi` и следуйте инструкциям мастера.

ПРИМЕЧАНИЕ

В названии файла `<lng>` - это язык компонента, `<version>` - номер версии компонента, а `<arch>` - целевая процессорная архитектура.

ОС Linux

ОБРАТИТЕ ВНИМАНИЕ

Команды на установку и удаление нужно запускать с правами суперпользователя.

Для установки SePlatform.HMI.SecurityConfigurator вызовите пакет с командой на установку в зависимости от используемого пакетного менеджера:

- rpm-пакет:

```
sudo rpm -i seplatform.hmi.securityconfigurator-<lng>-<version>.rpm
```

› deb-пакет:

```
sudo dpkg -i seplatform.hmi.securityconfigurator-<lng>-<version>.deb
```

ПРИМЕЧАНИЕ

В названии пакета `<lng>` - это язык компонента, а `<version>` - номер версии компонента.

Для удаления SePlatform.HMI.SecurityConfigurator вызовите команду на удаление приложения в зависимости от используемого пакетного менеджера:

› rpm-пакет:

```
sudo rpm -e seplatform.hmi.securityconfigurator
```

› deb-пакет:

```
sudo dpkg -r seplatform.hmi.securityconfigurator
```

1.3. Запуск приложения

SePlatform.HMI.SecurityConfigurator можно использовать как самостоятельное приложение, или встроить его в проект автоматизации, разработанный в SePlatform.HMI, в качестве внешнего модуля.

Чтобы запустить SePlatform.HMI.SecurityConfigurator как самостоятельное приложение, нажмите иконку приложения в меню Пуск.

Настройки самостоятельного приложения можно изменить в конфигурационном файле (стр. 25).

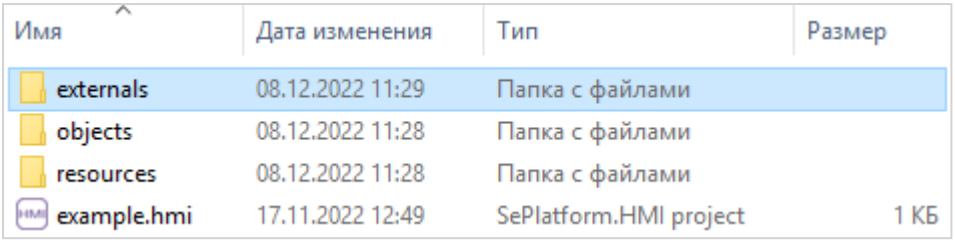
Встроить SePlatform.HMI.SecurityConfigurator в проект SePlatform.HMI

Чтобы встроить SePlatform.HMI.SecurityConfigurator в проект автоматизации, разработанный в SePlatform.HMI, подключите проект расширения в свой проект в виде внешнего модуля.

ОБРАТИТЕ ВНИМАНИЕ

Для встраивания SePlatform.HMI.SecurityConfigurator в проект SePlatform.HMI понадобится библиотека SePlatform.HMI.CommonLib.

1. Чтобы подключать проекты в виде внешних модулей, создайте в папке своего проекта папку с именем `externals`.



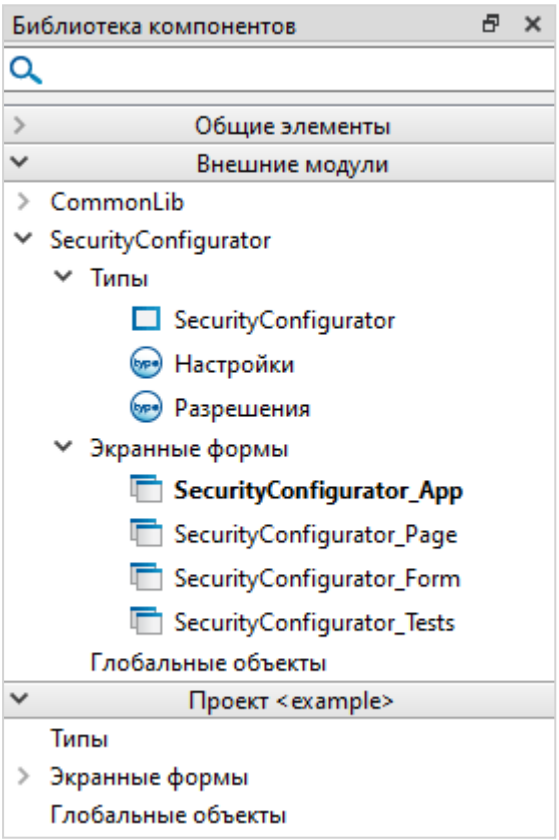
2. Перейдите к папке с расширениями SePlatform.HMI:

   - `C:\Program Files\SePlatform\SePlatform.HMI.Extensions` или `C:\Program Files (x86)\SePlatform\SePlatform.HMI.Extensions` (ОС Windows);
   - `/opt/SePlatform/SePlatform.HMI.Extensions` (ОС Linux).

Отсюда скопируйте папку `SecurityConfigurator` и папку библиотеки `CommonLib` в созданную ранее `externals`.

3. Запустите свой проект в Дизайнер SePlatform.HMI. В меню **Проект** на панели инструментов выберите **Обновить ссылки на внешние юниты**. В результате в библиотеке компонентов появятся юниты внешних модулей - **SecurityConfigurator** и **CommonLib**. Модуль **SecurityConfigurator** предоставляет следующие компоненты:

- Тип **SecurityConfigurator**, предназначенный для размещения на форме.
- Тип **SecurityConfigurator_Settings**, предназначенный для упрощения настройки экземпляров конфигуратора, создаваемых на основе типа **SecurityConfigurator** или указанных ниже форм.
- Основную экранную форму **SecurityConfigurator_App**, предназначенную для запуска окна конфигуратора в виде отдельного приложения.
- Экранную форму **SecurityConfigurator_Page**, предназначенную для открытия окна конфигуратора во фрейме.
- Экранную форму **SecurityConfigurator_Form**, предназначенную для открытия окна конфигуратора в виде отдельного окна.
- Экранную форму **SecurityConfigurator_Tests**, предназначенную для демонстрации примера встраивания конфигуратора в проект SePlatform.HMI.



Подробнее каждый компонент описан в Справочном руководстве.

Обновить SePlatform.HMI.SecurityConfigurator в проекте SePlatform.HMI

Если SePlatform.HMI.SecurityConfigurator уже встроен в проект в виде внешнего модуля, то при установке новой версии необходимо обновить файлы модуля в папке `externals` проекта. Для этого:

1. Установите нужную версию SePlatform.HMI.SecurityConfigurator.
2. Замените существующую папку `SecurityConfigurator` на папку `SecurityConfigurator`, расположенную в папке установки расширения:
   - `C:\Program Files\SePlatform\SePlatform.HMI.Extensions` или `C:\Program Files (x86)\SePlatform\SePlatform.HMI.Extensions` (ОС Windows);
   - `/opt/SePlatform/SePlatform.HMI.Extensions` (ОС Linux).
3. Если устанавливали новую версию SePlatform.HMI.CommonLib, не забудьте аналогично обновить файлы модуля в папке `externals` проекта.
4. Запустите свой проект в Дизайнер SePlatform.HMI. В меню **Проект** на панели инструментов выберите **Обновить ссылки на внешние юниты**. В результате внешние модули будут обновлены. Экранные формы **SecurityConfigurator**, уже добавленные в проект, обновятся автоматически.

1.4. Возможности приложения

В разделе продемонстрирована работа с возможностями приложения SePlatform.HMI.SecurityConfigurator. Для наглядности описан пример создания конфигурации SePlatform.Security.

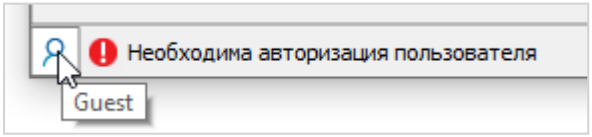
Предположим, согласно требованиям к примеру, все пользователи делятся на диспетчеров и операторов. Диспетчерам доступно управление резервуаром, а операторам - насосом. Кроме того, существует роль начальника участка, которому доступно управление обоими объектами.

Тогда, чтобы создать нужную конфигурацию, необходимо:

1. Создать две группы (стр. 11) пользователей - **«Диспетчеры»** и **«Операторы»**.
2. Создать права (стр. 12) на управление резервуаром и насосом и назначить их (стр. 14) соответствующим группам пользователей.
3. Создать роль (стр. 15) начальника участка.
4. Создать учетные записи (стр. 16) пользователей проекта и поместить их в группы, а также назначить роль.

1.4.1. Вход с учетными данными

Чтобы приступить к работе, необходимо авторизоваться. Для авторизации нажмите на иконку в левом нижнем углу.

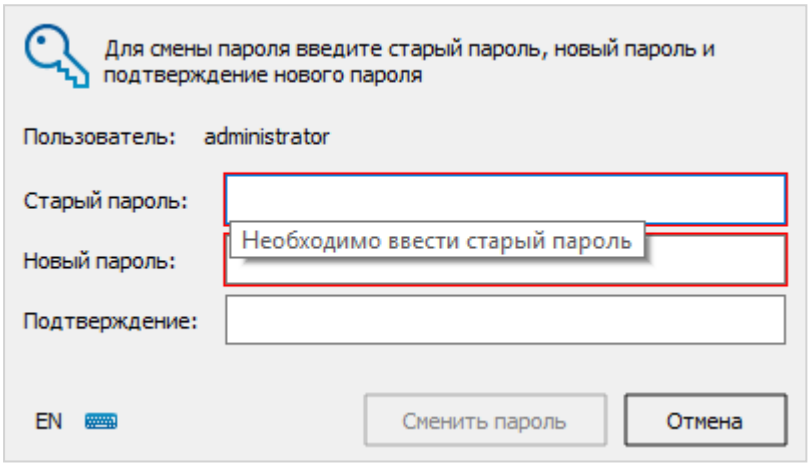


ОБРАТИТЕ ВНИМАНИЕ

По умолчанию, если конфигурация SePlatform.Security не создана, каталог на LDAP-сервере и учетная запись администратора SePlatform.Security создадутся при первом запуске конфигуратора. Имя каталога - **`SePlatform.Security`**. Учетные данные администратора, обладающего правами на просмотр и изменение конфигурации:

- логин - **«administrator»**;
- пароль - такой же, какой был введен при установке LDAP-сервера в составе SePlatform.Security (если этот шаг был пропущен, стандартное значение пароля - **«secret»**). Далее этот пароль нужно будет обновить в целях безопасности.

Введите указанные учетные данные и нажмите **Войти в систему**. Появится диалоговое окно, требующее обновления пароля. Нажмите **OK** и в открывшемся окне введите новый пароль.



Если же необходимо конфигурировать созданный ранее каталог и использовать имеющуюся учетную запись администратора, настройте Агент SePlatform.Security. Настройка Агент SePlatform.Security описана в документе на подсистему безопасности SePlatform.Security.

Если введены учетные данные пользователя, обладающего правами на просмотр и изменение конфигурации, соответствующие действия будут доступны. В противном случае доступ будет отклонен, и в окне конфигуратора появится сообщение об этом.

ПРИМЕЧАНИЕ

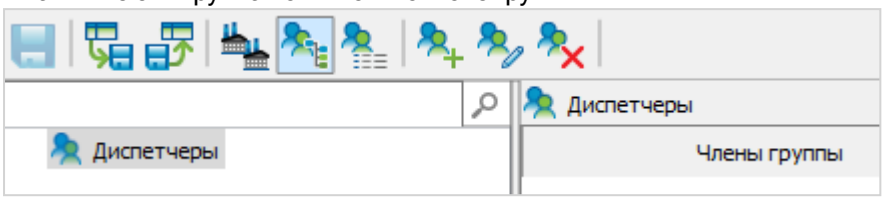
Вы можете создать собственную учетную запись администратора, наделив его правами на просмотр и изменение конфигурации, а затем удалить учетную запись **«administrator»**.

1.4.2. Создание и редактирование групп пользователей

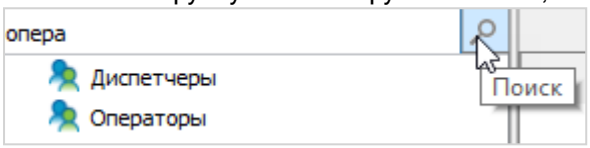
Пользователей можно объединять в группы для удобства. Это помогает назначать одинаковые разрешения и запреты нескольким пользователям одновременно.

Создадим две группы пользователей: **«Диспетчеры»** и **«Операторы»**.
Создание и редактирование групп ведется в окне просмотра групп. Чтобы открыть окно, нажмите **Показать группы пользователей**.

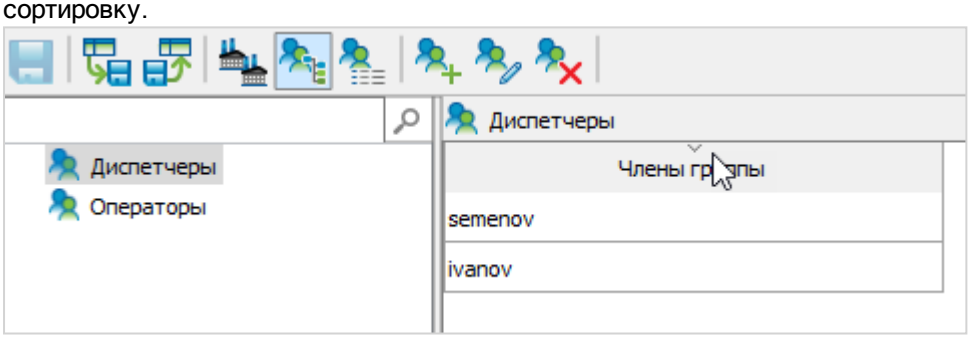
Чтобы создать новую группу, нажмите **Добавить группу** . В открывшемся окне введите название группы и нажмите **ОК**. Группа появится в списке групп.



Аналогично создайте группу **«Операторы»**.
Чтобы редактировать группу, нажмите **Редактировать группу** или дважды кликните по строке группы в списке.
Чтобы найти группу в списке групп по имени, воспользуйтесь панелью поиска над списком.



Для сортировки списка пользователей, состоящих в группе, нажмите на заголовок списка **Члены группы**. Первое нажатие сортирует список по возрастанию, второе - по убыванию, третье нажатие отключает сортировку.



Специальные команды редактирования групп

Команда	Кнопка	Описание
Блокировать группу пользователей		Используется, когда необходимо ограничить доступ в систему всем пользователям, состоящим в группе. Пока группа заблокирована, попытки входа участников отклоняются подсистемой безопасности. Чтобы разблокировать заблокированную группу, нажмите . ОБРАТИТЕ ВНИМАНИЕ Блокировка группы, в которой находится текущий пользователь, невозможна.

1.4.3. Создание приложений и прав

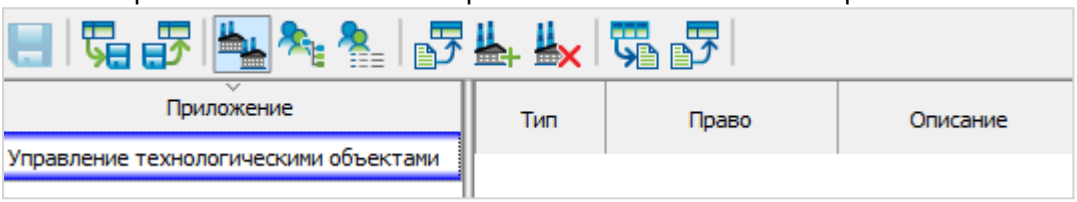
Возможности пользователей в проекте определяются наличием у них разрешений и запретов на определенные действия. Информация о том, разрешено или запрещено пользователю какое-либо действие, хранится в праве. Для удобства права сгруппированы в приложения. Подробнее об этом в Руководстве пользователя подсистемы безопасности SePlatform.Security.

Создание и редактирование приложений и прав ведется в окне просмотра приложений. Чтобы открыть окно, нажмите **Показать список приложений**.

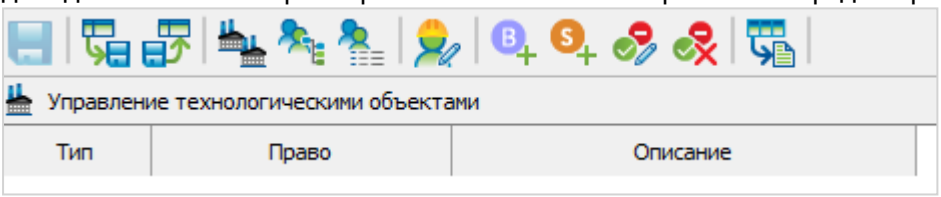
Приложение можно:

- создать в окне редактирования приложений;
- импортировать из файла. Подробнее об этом в 1.4.8. Безопасность в компонентах Систэм Платформ (стр. 22).

Чтобы создать новое приложение, нажмите **Добавить приложение**  . В открывшемся окне введите название приложения и нажмите **ОК**. Приложение появится в списке приложений.



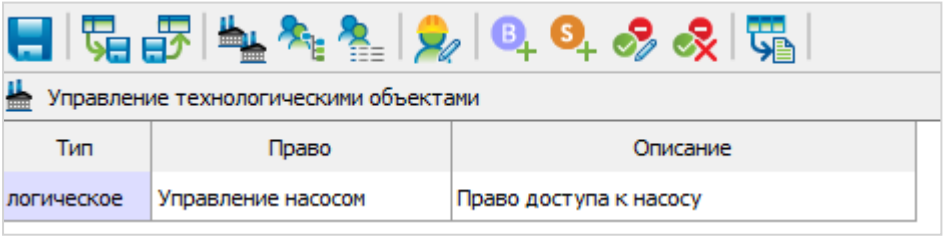
Теперь в приложении необходимо создать права. Для этого нажмите **Редактировать приложение**  или дважды кликните по строке приложения в списке. Откроется окно редактирования приложения.



Чтобы разграничить доступ будущих пользователей к технологическим объектам, необходимо создать два логических права:

- одно предоставляет доступ к управлению резервуаром;
- другое предоставляет доступ к управлению насосом.

Для этого в окне редактирования приложения нажмите **Добавить логическое право**  . В открывшемся окне введите название права и нажмите **Добавить**. Право будет создано и появится в списке прав приложения.



Нажмите **Сохранить изменения**, чтобы подтвердить внесенные изменения.
Аналогичным образом создайте еще одно логическое право **«Управление резервуаром»**.

Экспорт и импорт приложений

В окне просмотра приложений доступен просмотр таблицы с информацией о правах приложения, выбранного из списка. Эту таблицу можно сохранить в файл. Для этого в окне просмотра приложений нажмите **Экспорт в файл...**  . Откроется диалоговое окно, где будет предложено выбрать полный путь к папке для хранения файла, имя файла и его расширение: `*.csv` или `*.xlsx` (о создании и применении файлов с расширением `*.json` написано ниже). Укажите требуемые параметры и нажмите **Сохранить**.

Приложение вместе с его правами можно сохранить в файл-шаблон. Такой файл можно использовать для импорта приложения в конфигурацию SePlatform.Security.

› Чтобы сохранить шаблон приложения, выберите нужное приложение из списка и нажмите **Экспорт в файл...**  . В открывшемся окне укажите путь к папке для хранения файла, имя файла и расширение `*.json`, а затем нажмите **Сохранить**. Файл появится в указанном расположении.

› Чтобы импортировать ранее сохраненный шаблон приложения, откройте окно просмотра приложений и нажмите **Импортировать приложение из файла...**  . В открывшемся окне перейдите к расположению файла и откройте его. Приложение появится в списке приложений.

1.4.4. Назначение прав

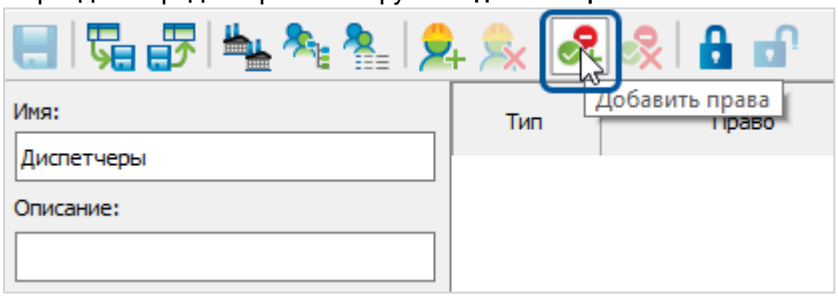
ПРИМЕЧАНИЕ

Право может быть назначено:

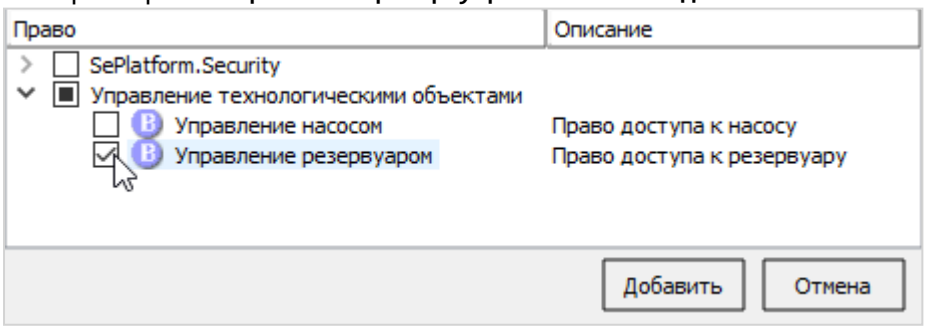
- пользователю лично - в окне редактирования учетной записи пользователя;
- группе пользователей - в окне редактирования группы;
- роли - в окне редактирования роли.

В результате эффективное значение права для пользователя зависит от того, какое значение права назначено ему лично, в каких группах он состоит и какие роли ему назначены. Подробнее об этом в 1.4.7. Получение эффективных значений прав (стр. 21) (стр. 21).

Назначим права созданным ранее группам.
Перейдите к редактированию группы **«Диспетчеры»**. Чтобы назначить право группе нажмите **Добавить права**.



Выберите право **«Управление резервуаром»** и нажмите **Добавить**.



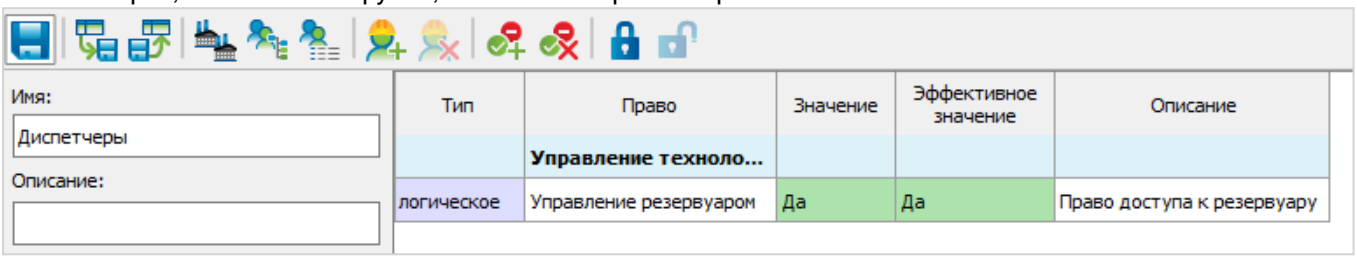
ПРИМЕЧАНИЕ

В окне выбора прав можно выбрать несколько прав одновременно.

ПРИМЕЧАНИЕ

Приложение **SePlatform.Security** - это системное приложение, оно содержит системные права. Их можно назначить пользователю, например, чтобы разрешить просмотр и редактирование конфигурации, или ограничить длительность сессии пользователя. Подробнее каждое право описано в 1.6.1. Права стандартного приложения SePlatform.Security (стр. 27).

В списке прав, назначенных группе, появится выбранное право.

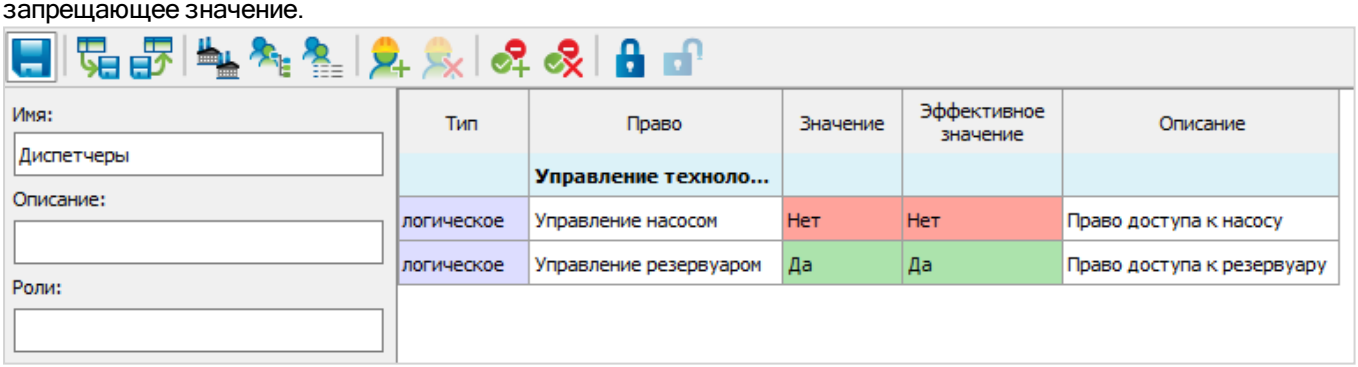


Значение добавляемого права по умолчанию - **«Да»**.

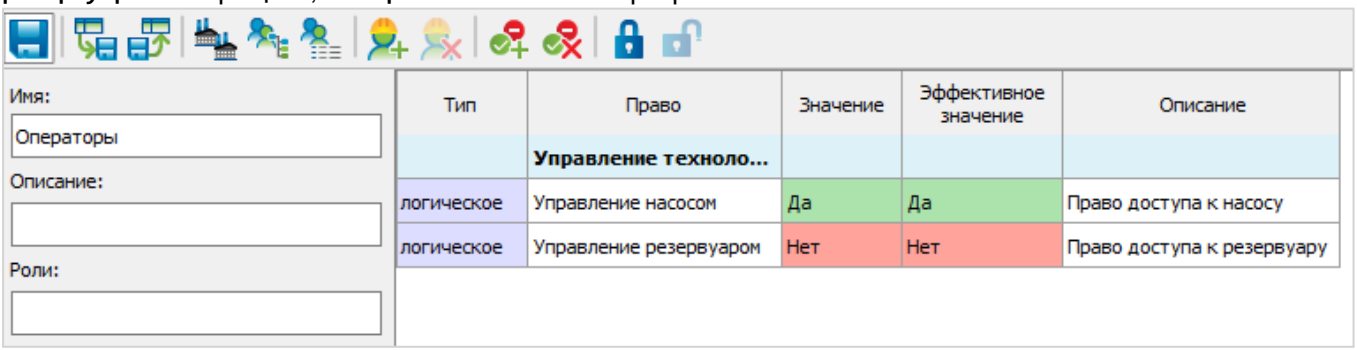
ОБРАТИТЕ ВНИМАНИЕ

Чтобы изменить значение права, дважды кликните в ячейке столбца **Значение**.

Оставьте разрешающее значение добавленного права, поскольку пользователям данной группы разрешено **«Управление резервуаром»**.
Сделаем права доступа к оборудованию взаимоисключающими: если есть доступ к резервуару, то нет доступа к насосу, и наоборот. Для этого назначьте группе право **«Управление насосом»** и укажите для него запрещающее значение.



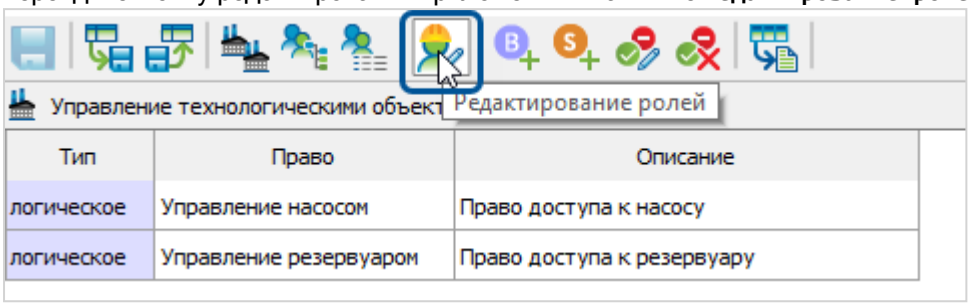
Для группы **«Операторы»** следует назначить те же права, но значения указать наоборот: **«Управление резервуаром»** запрещено, а **«Управление насосом»** разрешено.



1.4.5. Создание ролей

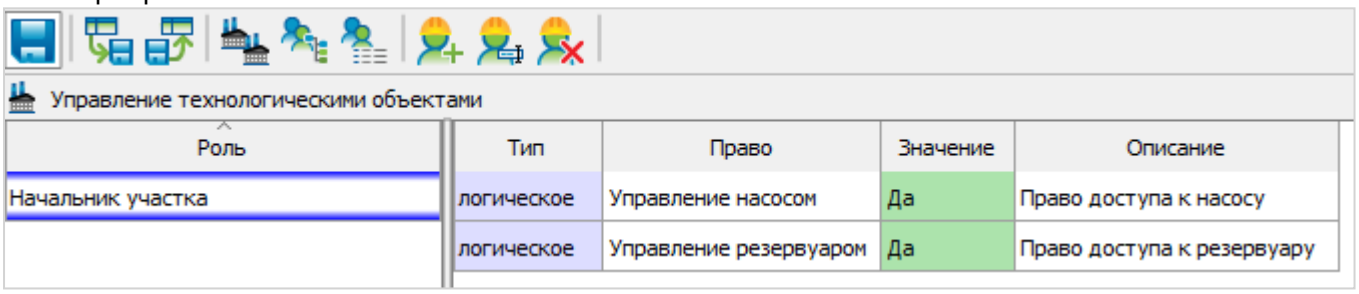
Внутри приложения можно создать роль. Роль - это совокупность значений каждого права приложения. Роль может быть назначена как пользователю, так и группе.

Создадим роль начальника участка, имеющего права на управление обоими технологическими объектами: и насосом, и резервуаром.
Создание и редактирование списка ролей ведется в окне редактирования ролей. Чтобы открыть окно, перейдите к окну редактирования приложения и нажмите **Редактирование ролей**.



Тип	Право	Описание
логическое	Управление насосом	Право доступа к насосу
логическое	Управление резервуаром	Право доступа к резервуару

Откроется окно редактирования ролей. Чтобы создать новую роль, нажмите **Добавить роль**  . В открывшемся окне введите название роли и нажмите **ОК**. Роль появится в списке ролей. Назначение прав роли происходит автоматически, так как роль относится к приложению. Оставьте разрешающие значения для обоих прав роли.



Роль	Тип	Право	Значение	Описание
Начальник участка	логическое	Управление насосом	Да	Право доступа к насосу
	логическое	Управление резервуаром	Да	Право доступа к резервуару

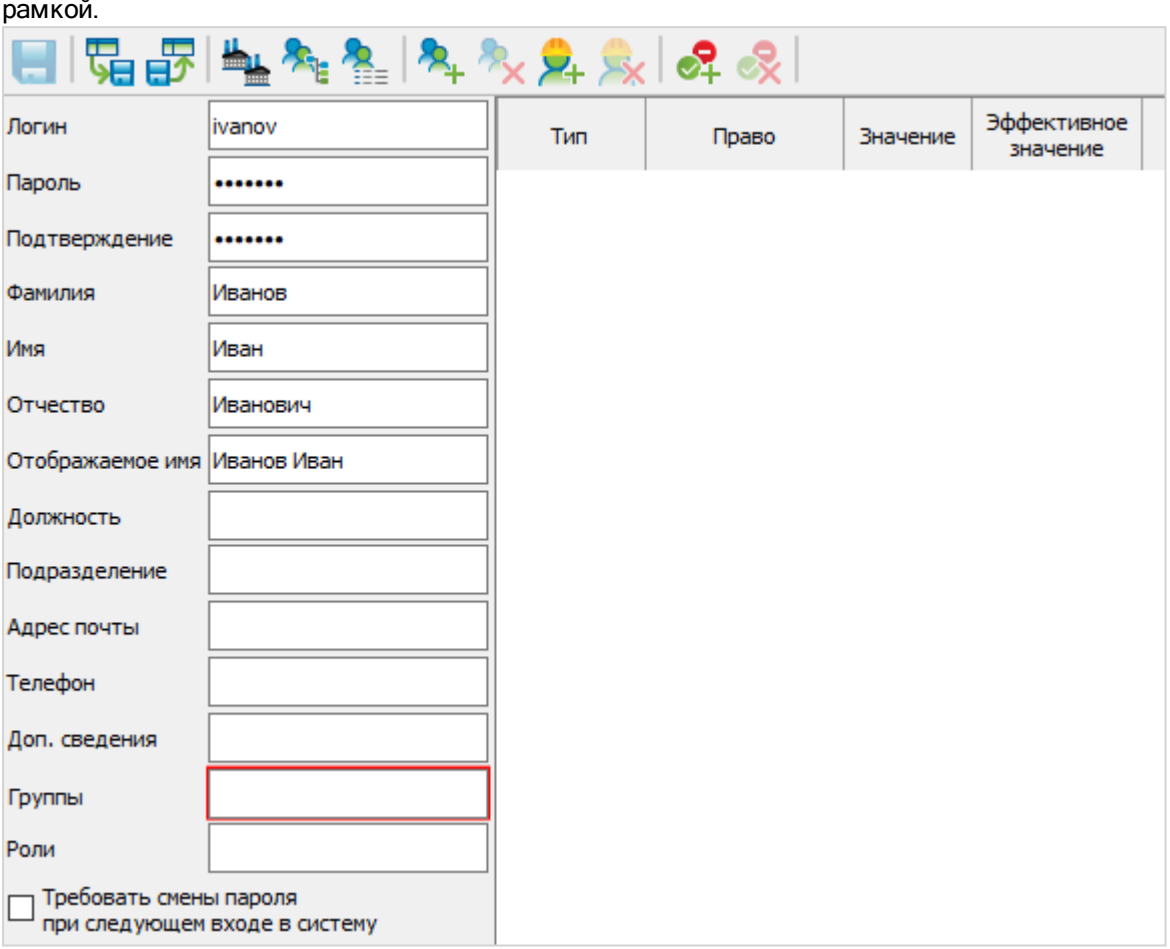
1.4.6. Создание и редактирование учетных записей пользователей

Чтобы пользователи могли получить доступ к возможностям проекта, каждому из них необходимо создать личную учетную запись.

Создадим новую учетную запись пользователя.
Создание и редактирование списка учетных записей ведется в окне просмотра учетных записей. Чтобы открыть окно, нажмите **Показать список пользователей**.

Появится список всех учетных записей, существующих в подсистеме безопасности SePlatform.Security. Пока среди них находится только администратор.

Чтобы создать новую учетную запись нажмите **Добавить учётную запись пользователя**  . Откроется окно создания и редактирования учетной записи. Заполните все необходимые поля, выделенные красной рамкой.

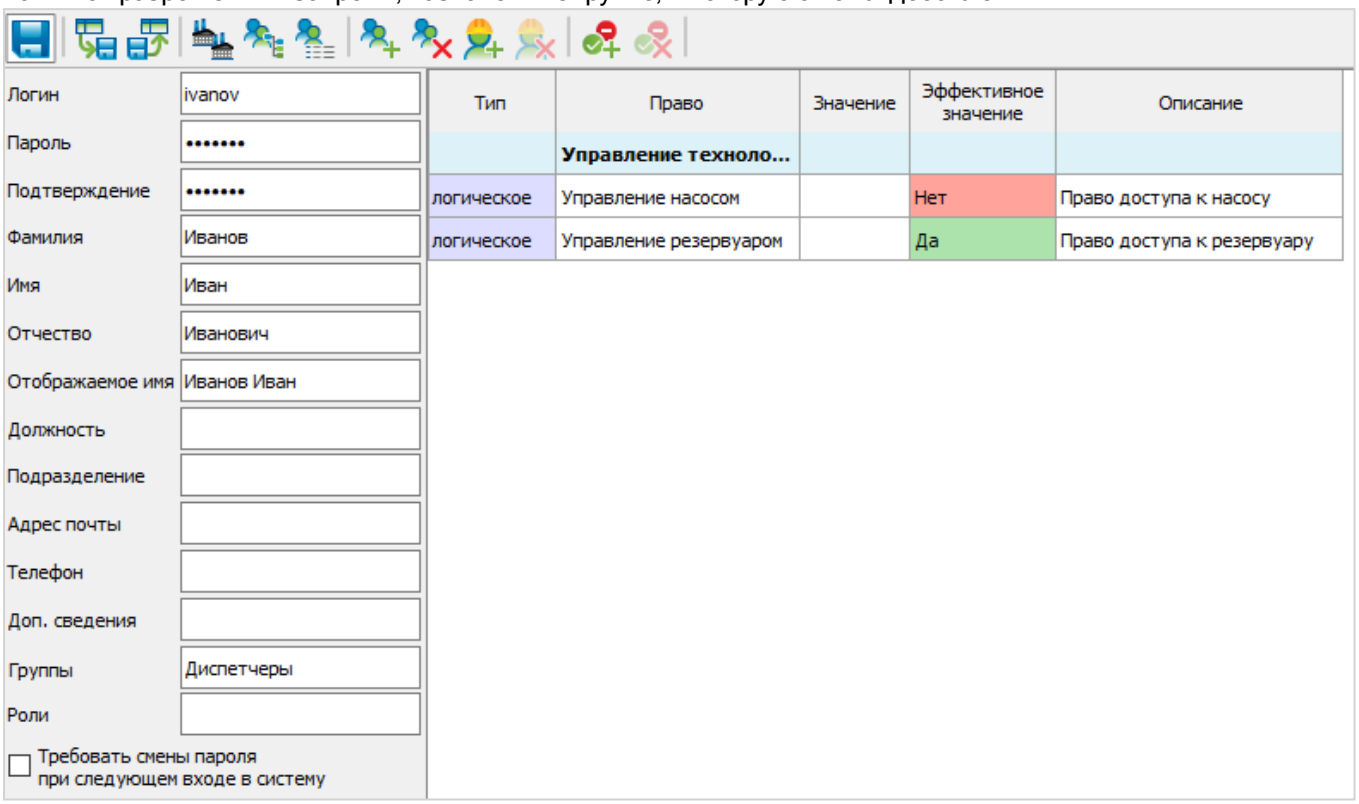


ПРИМЕЧАНИЕ

Поле **Отображаемое имя** заполняется автоматически, его значение состоит из введенных фамилии, имени и отчества. Однако значение отображаемого имени можно менять.

Добавим пользователя в предназначенную для него группу. Для этого нажмите **Добавить в группу**  .

Откроется окно выбора группы. Выберите группу **«Диспетчеры»** и нажмите **Добавить**. У пользователя появятся разрешения и запреты, назначенные группе, в которую он был добавлен.

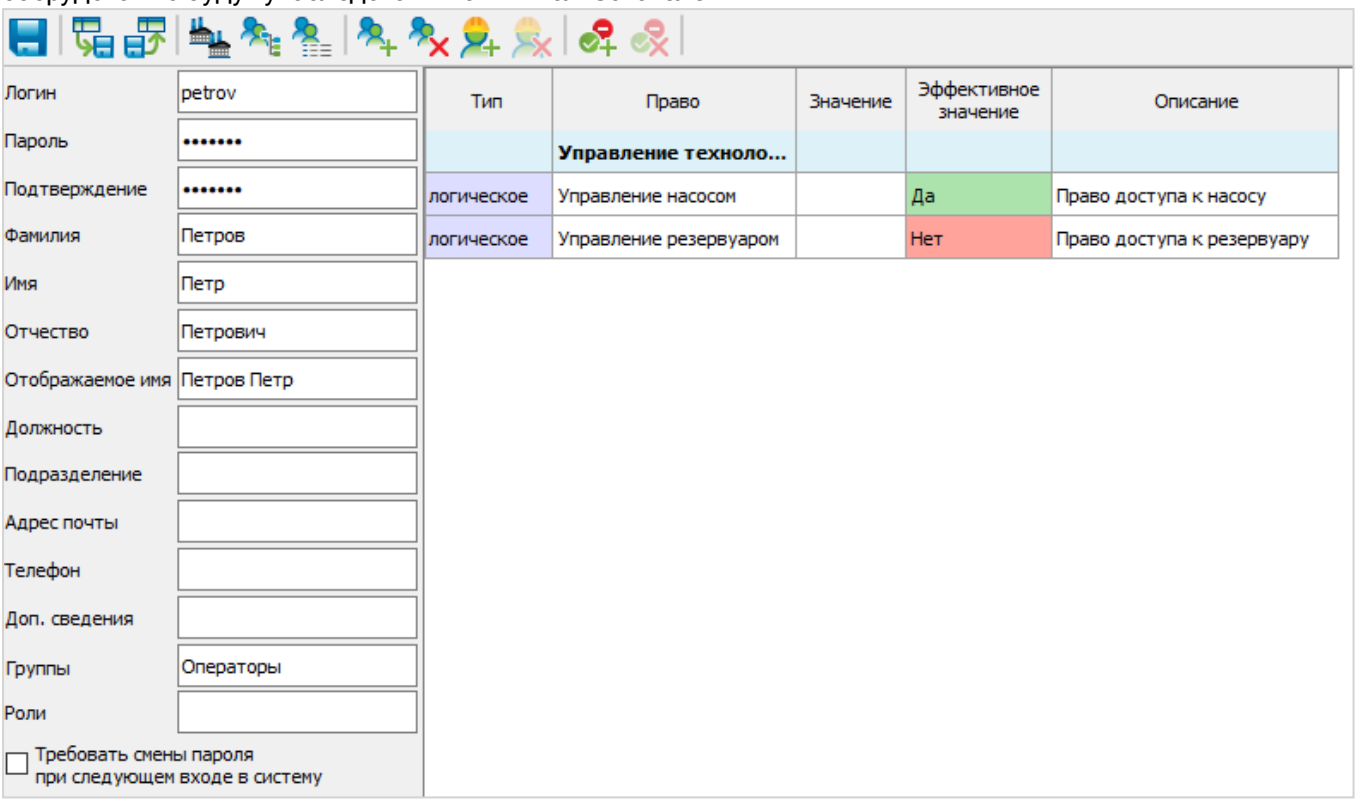


Значения прав записаны в столбец **Эффективное значение**. Это связано с тем, что права унаследованы от группы. Подробнее об эффективных значениях прав в 1.4.7. Получение эффективных значений прав (стр. 21).

ПРИМЕЧАНИЕ

Количество групп, в которые пользователь может быть добавлен одновременно, регулируется свойством **UserInOnlyOneGroup** компонента 2.2. Настройки (стр. 31) или настройками приложения (стр. 25).

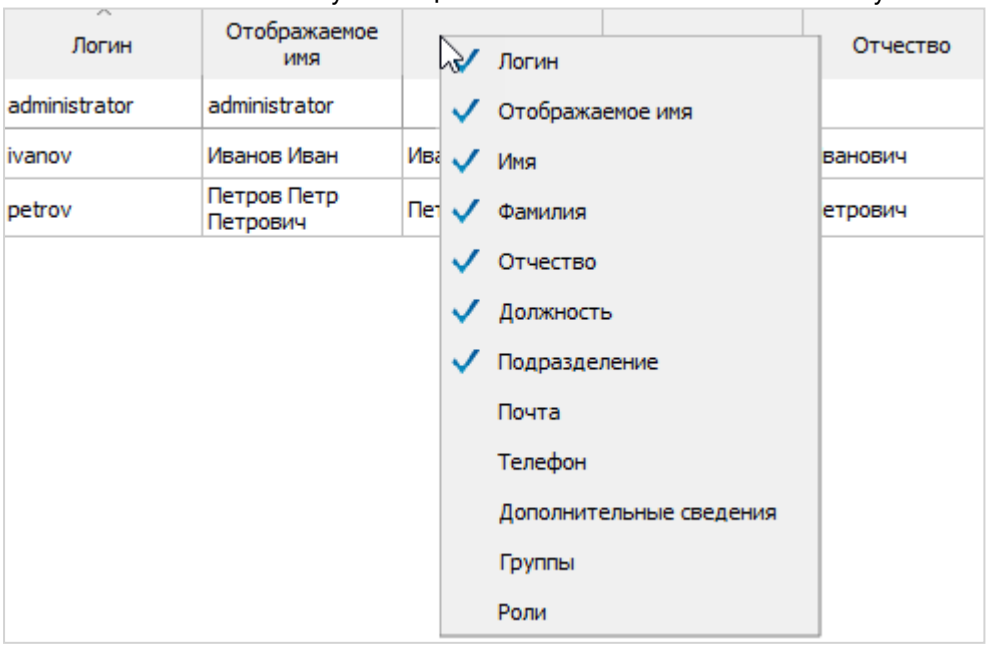
Создайте еще одного пользователя и добавьте его в группу **«Операторы»**. Значения прав доступа к оборудованию будут унаследованы новым пользователем.



Чтобы удалить учетную запись пользователя, в окне просмотра пользователей выберите пользователя в таблице и нажмите кнопку **Удалить учётную запись пользователя** .

Чтобы вернуться к окну редактирования учетной записи нажмите **Редактировать учётную запись пользователя** или дважды кликните по строке нужной учетной записи в таблице.

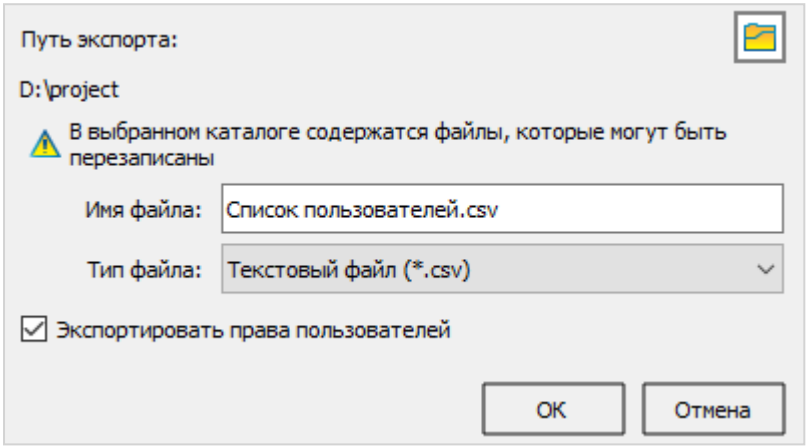
В таблице, отображаемой в окне просмотра учетных записей, можно изменить набор столбцов. Для этого кликните ПКМ по заголовку таблицы и в контекстном меню отметьте нужные столбцы.



Экспорт списка пользователей и списков их эффективных прав

Таблицу со списком пользователей можно сохранить в файл. Для этого нажмите **Экспорт в файл...** .

Откроется диалоговое окно, где будет предложено выбрать расположение, имя файла и его расширение: `*.csv` или `*.xlsx`. Здесь же можно указать, следует ли экспортировать списки прав каждого пользователя в отдельные файлы с таким же расширением, как у файла списка пользователей. Чтобы изменить расположение файла, нажмите **Выбрать папку** .



Укажите требуемые параметры и нажмите **Сохранить**.

ПРИМЕЧАНИЕ

В файл со списком пользователей сохраняются те данные, которые отображаются в таблице в окне просмотра учетных записей (логин, имя, фамилия и пр.). Чтобы изменить набор данных в сохраняемом файле, измените видимость столбцов в таблице. Также можно изменить ширину столбцов.

Специальные команды редактирования учетных записей

Команда	Кнопка	Описание
Блокировать учетную запись пользователя		Используется, когда необходимо ограничить доступ пользователя в систему. Пока пользователь заблокирован, попытки входа отклоняются подсистемой безопасности. Чтобы разблокировать заблокированную учетную запись, нажмите . ОБРАТИТЕ ВНИМАНИЕ Блокировка учетной записи текущего пользователя невозможна.

Команда	Кнопка	Описание
Завершить сессию пользователя на указанных АРМ.		Предоставляет администратору возможность завершить сессии выбранного пользователя на указанных АРМ. Наличие команды связано со свойством **DomainNodesList** компонента **`SecurityConfigurator`**. Подробнее свойство описано в Справочном руководстве (стр. 30)

1.4.7. Получение эффективных значений прав

Значение одного и того же права может быть назначено:

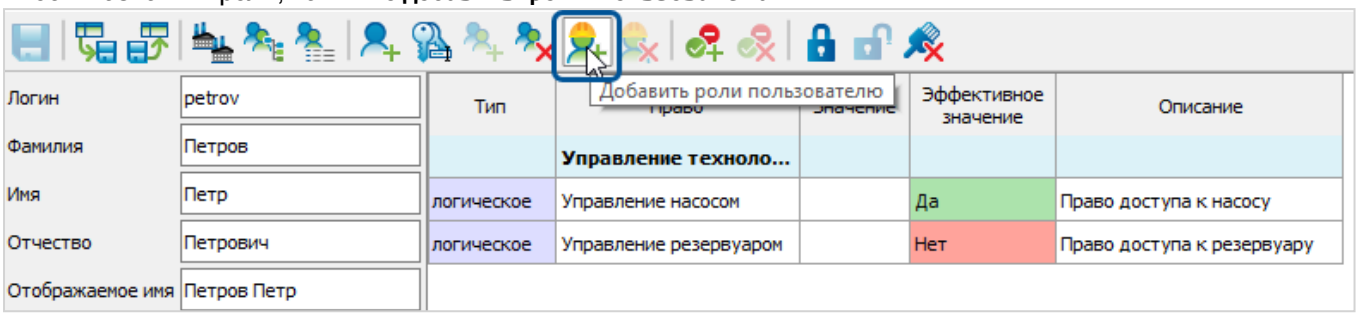
- пользователю лично;
- группе пользователей;
- роли.

Значение права для пользователя зависит от того, в каких группах он состоит, какие роли ему назначены, и какое значение права назначено пользователю лично. Итоговое значение называется эффективным значением права.

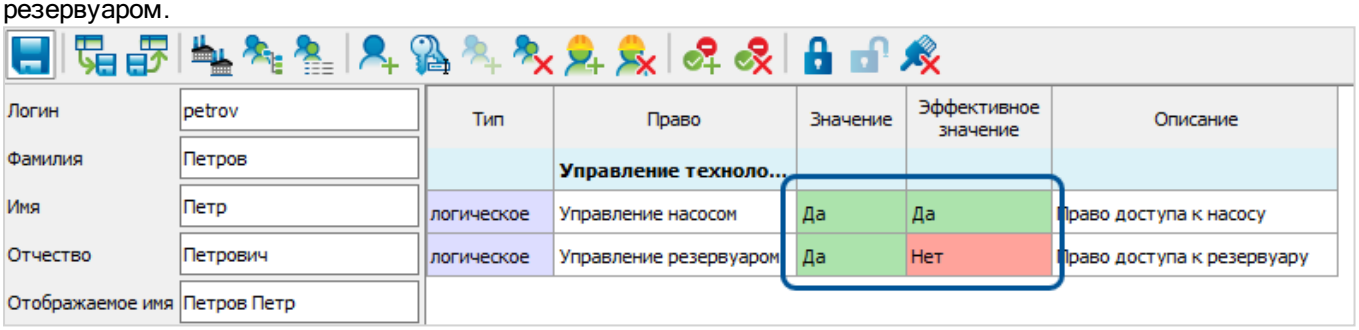
Правила определения эффективного значения права:

- Для логического права:
  - если есть хоть одно разрешающее значение и нет запрещающих, эффективное значение разрешающее;
  - если есть хоть одно запрещающее значение, эффективное значение запрещающее.
- Для строковых прав эффективное значение складывается из всех наследованных прав. Строковые права отображаются списком.
- Эффективные значения для системных прав SePlatform.Security приведены в 1.6.1. Права стандартного приложения SePlatform.Security (стр. 27).

Допустим, пользователь Петров Петр является одновременно и оператором, и начальником участка. Перейдите к редактированию учетной записи этого пользователя и назначьте ему роль начальника участка. Чтобы назначить роль, нажмите **Добавить роли пользователю**.



Пользователь унаследует разрешающие значения прав роли, но ему по-прежнему будет запрещено управлять резервуаром, так как он находится в группе **Операторы**. Назначьте права на управление состоянием оборудования пользователю лично. Эффективным значением также будет запрет на управление резервуаром.



Разрешите управление резервуаром группе **Операторы**. Тогда эффективным значением для пользователя станет разрешение на управление резервуаром, так как управление разрешено:

- группе **Операторы**, в которой состоит пользователь;
- роли **Начальник участка**, которая назначена пользователю;
- пользователю лично.

1.4.8. Безопасность в компонентах Систэм Платформ

Подсистема безопасности SePlatform.Security дает возможность разграничивать возможности пользователей в некоторых компонентах Систэм Платформ:

- SePlatform.HMI.Alarms;
- SePlatform.HMI.Trends;
- SePlatform.HMI.IntegrityControl;
- SePlatform.HMI.SetPoints;
- SePlatform.HMI.Statistics;
- SePlatform.Development Studio.

Подробнее о том, как именно активировать сервис безопасности, читайте в документах на соответствующие компоненты.
После того, как сервис безопасности активирован, необходимо назначить пользователям права на использование возможностей компонентов. Для этого необходимы приложения:

- **`Alarms`** для SePlatform.HMI.Alarms;
- **`Trends`** для SePlatform.HMI.Trends;
- **`IntegrityControl`** для SePlatform.HMI.IntegrityControl;
- **`SetPoints`** для SePlatform.HMI.SetPoints;

- **`Statistics`** для SePlatform.HMI.Statistics;
- **`DevStudio`** для SePlatform.Development Studio.

Шаблоны этих приложений поставляются вместе с дистрибутивом SePlatform.HMI.SecurityConfigurator и находятся в папке:

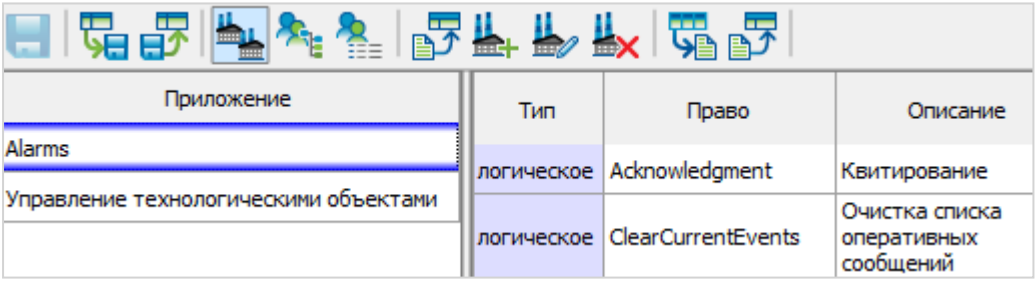
- `C:\Program Files\SePlatform\SePlatform.HMI.SecurityConfigurator\resources\Security_Templates` или `C:\Program Files (x86)\SePlatform\SePlatform.HMI.SecurityConfigurator\resources\Security_Templates` для ОС Windows;
- `/opt/SePlatform/SePlatform.HMI.SecurityConfigurator/resources/Security_Templates` для ОС Linux.

Чтобы использовать приложения в своих проектах, импортируйте приложения в конфигурацию SePlatform.Security. Для этого откройте окно просмотра приложений и нажмите **Импортировать приложение из файла**  . Откроется окно импорта шаблона приложения. Перейдите к расположению шаблонов, выберите нужный, и нажмите **Открыть**.

ПРИМЕЧАНИЕ

Путь к папке шаблонов приложений можно указать в свойстве AppTemplatesPath компонента 2.2. Настройки (стр. 31) или в настройках приложения (стр. 25). Если значение не указано, то по умолчанию используется путь к папке `Security_Templates` в папке проекта.

Приложение появится в списке приложений.

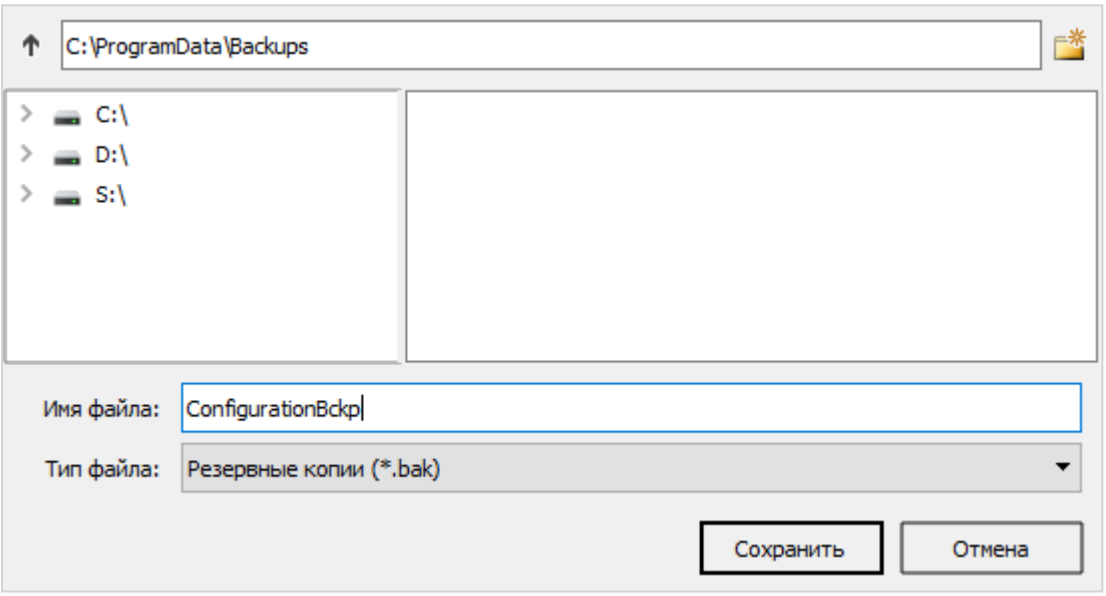


1.4.9. Резервное копирование конфигурации

Для сохранения текущей конфигурации подсистемы безопасности можно создать ее резервную копию. При необходимости сохраненную конфигурацию можно восстановить из резервной копии.

Чтобы создать резервную копию текущей конфигурации, нажмите **Сохранить резервную копию конфигурации**.

Откроется диалоговое окно, где будет предложено ввести полный путь к папке для хранения резервной копии и имя резервной копии. Укажите оба параметра и нажмите **Сохранить**.



- Чтобы перейти к папке на уровень выше, нажмите ↑.
- Чтобы создать в указанном расположении новую папку, нажмите .

ОБРАТИТЕ ВНИМАНИЕ

Для создания резервной копии нужно обладать правами на чтение, создание и изменение файлов в указанной папке.

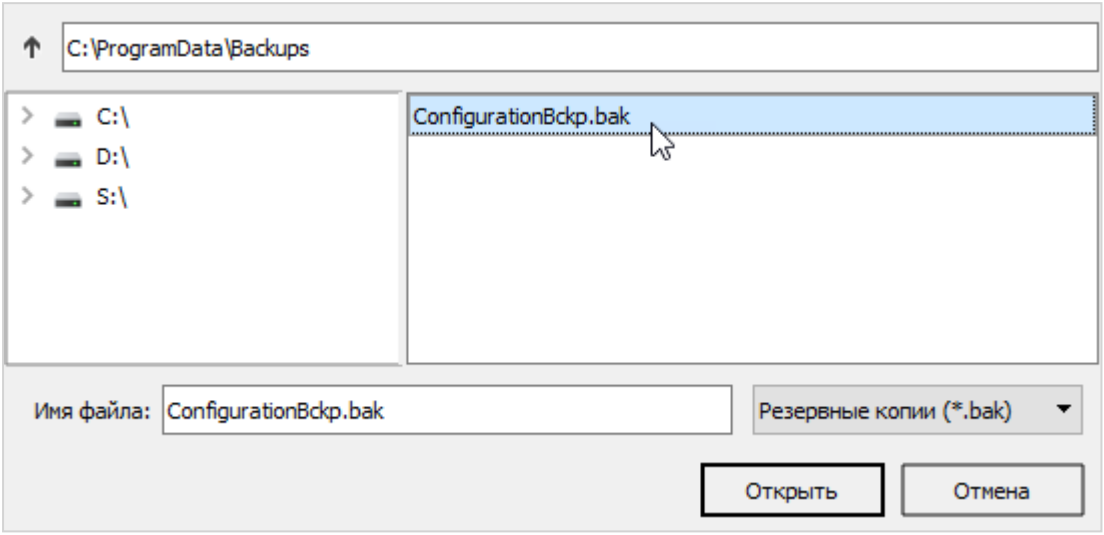
ПРИМЕЧАНИЕ

Путь к папке для хранения резервных копий конфигурации указывается в свойстве BackupsPath компонента **SecurityConfigurator**. Если значение не указано, то по умолчанию используется путь к папке `Backups`, создающейся в папке проекта при первом сохранении резервной копии. Подробнее свойство описано в Справочном руководстве (стр. 30).

Теперь восстановите сохраненную конфигурацию из резервной копии. Для наглядности удалите любую учетную запись, кроме **«administrator»**, и приложение **«Управление состоянием технологического оборудования»**.

Чтобы восстановить конфигурацию из резервной копии, нажмите **Восстановить конфигурацию из резервной копии**.

Откроется диалоговое окно, где будет предложено ввести полный путь к файлу резервной копии и полное имя резервной копии. Укажите оба параметра и нажмите **Открыть**.



ОБРАТИТЕ ВНИМАНИЕ

Для восстановления резервной копии нужно обладать правами на чтение файлов в указанной папке.

Удаленная учетная запись вновь появится в списке учетных записей, а удаленное приложение - в списке приложений.

1.5. Настройка приложения в конфигурационных файлах

Настройки функций приложения

Некоторые функции приложения можно настроить, изменив конфигурационный файл `app_settings.json`, расположенный в:

- `C:\ProgramData\SePlatform\HMI.SecurityConfigurator` для ОС Windows;
- `/home/<user>/SePlatform/HMI.SecurityConfigurator` для ОС Linux.

Пример такого файла:

```
{
 "UserInAtLeastOneGroup": true,
 "UserInOnlyOneGroup": false,
 "AppTemplatesPath": "C:\\Program
Files\\SePlatform\\SePlatform.HMI.SecurityConfigurator\\resources\\Security_
Templates",
 "BackupsPath": "C:\\ProgramData\\Backups",
 "DomainNodes": "",
 "ScreenKeyboard":
 {
```

```
  "Enabled": false,
  "ProgramPath": "",
  "Arguments": ""
 }
}
```

Параметры настроек из файла совпадают со свойствами компонента 2.2. Настройки (стр. 31). Кратко параметры описаны ниже.

Параметр	Назначение
`UserInAtLeastOneGroup`	Регулирует обязательность добавления пользователя в группу.
`UserInOnlyOneGroup`	Регулирует количество групп, в которых пользователь может состоять одновременно.
`AppTemplatesPath`	Полный путь к папке для хранения шаблонов приложений.
`BackupsPath`	Полный путь к папке для хранения резервных копий конфигурации подсистемы безопасности.
`DomainNodes`	Список имен АРМ, на которых можно завершить сессию пользователя.
`ScreenKeyboard`	Настройки использования экранной клавиатуры, где: › `Enabled` - настройка видимости кнопки вызова экранной клавиатуры. › `ProgramPath` - полный путь к программе экранной клавиатуры. Можно не указывать. По умолчанию будет использоваться: › в Windows - `seplatform.hmi.keyboard.exe` (поставляется вместе с дистрибутивом SePlatform.HMI). › в Linux - `/usr/bin/fly-vkbd`. › `Arguments` - аргументы запуска программы экранной клавиатуры. Зависят от используемой программы.

Настройки внешнего вида приложения

Информация о приложении сохраняется в конфигурационные файлы. Это необходимо для того, чтобы сохранять внешний вид и положение окна SePlatform.HMI.SecurityConfigurator при перезапуске приложения.

Имя файла	Назначение
`session.json`	В файл записываются данные о положении и размере окна приложения в последней сессии.

Имя файла	Назначение
`settings.json`	Хранит информацию о внешнем виде приложения: › ширине и видимости таблиц (пользователей, приложений и пр.) и их столбцов; › ширине списков (приложений, групп и пр.), расположенных в левой части окна приложения. Также здесь хранятся пути: › к папке, выбранной для экспорта файлов `*.csv` или `*.xlsx`; › к папке, из которой импортируются шаблоны приложений.

Чтобы ознакомиться с файлами, перейдите к их расположению:

- `C:\Users\<user>\SePlatform\HMI.SecurityConfigurator` для ОС Windows;
- `/home/<user>/SePlatform/HMI.SecurityConfigurator` для ОС Linux.

1.6. Приложения

1.6.1. Права стандартного приложения SePlatform.Security

Право	Краткое описание	Описание
`AttempsTimeOut`	Таймаут при превышении количества попыток входа, мин	Длительность блокировки пользователя при превышении количества неудачных попыток, указанных в **`MaxAttempsCount`**.
`ConfigurationAccess`	Редактирование конфигурации	Предоставляет доступ к редактированию конфигурации SePlatform.Security. Этим правом наделяется администратор SePlatform.Security.
`EditSettings`	Изменение настроек	Предоставляет доступ к настройкам SePlatform.HMI.SecurityConfigurator. Не применяется в текущей версии SePlatform.HMI.SecurityConfigurator.
`InteractiveLogon`	Интерактивный вход	Разрешает/запрещает пользователю вход. Устаревшее право SePlatform.Security, функцию которого выполняет блокировка. Для разрешения или запрета входа используйте блокировку учетной записи пользователя (см. Специальные команды редактирования учетных записей (стр. 16))

Право	Краткое описание	Описание
LowerCount	Количество в пароле символов в нижнем регистре	Устанавливает минимально допустимое количество символов в нижнем регистре в пароле.
MaxAttempsCount	Количество попыток входа, шт	Устанавливает количество неудачных попыток входа для пользователя. Если пользователь не войдет за указанное количество попыток, то блокируется на время, указанное в **AttempsTimeOut**.
MaxIdleTime	Максимальное время бездействия, мин	Устанавливает время бездействия пользователя. Таймер сбрасывается при каждом взаимодействии пользователя с АРМ - щелчком или движением мыши, вводом текста с клавиатуры и т.д. Если же за указанное время пользователь не взаимодействует с АРМ, происходит автоматический выход пользователя из системы. Эффективным значением права является максимальное значение.
NumberCount	Количество цифровых символов в пароле	Устанавливает минимально допустимое количество цифр в пароле.
PasswordAge	Срок действия пароля, дней	Устанавливает границы срока действия пароля. До истечения минимального срока действия обновить пароль нельзя. После истечения максимального срока действия пароля попытки входа со старыми учетными данными будут отклоняться. Эффективным значением минимального срока является максимальное значение. Эффективным значением максимального срока является минимальное значение.
PasswordComplexity	Сложность пароля	Обязательность использования в пароле следующих видов символов: › цифры; › буквы нижнего регистра; › буквы верхнего регистра; › специальные символы.
PasswordMinLength	Минимальная длина пароля	Устанавливает минимально допустимое количество символов в пароле.

Право	Краткое описание	Описание
PasswordNotifyForChange	Уведомление о смене пароля, дней	Позволяет создать напоминание об истечении срока действия пароля для пользователя. За указанное до истечения пароля время будет отправлено напоминание о скором истечении срока действия пароля. Эффективным значением является максимальное значение.
PasswordsInHistory	Количество паролей в истории	Устанавливает количество хранимых в истории паролей. Обновить пароль на такой же, как в истории паролей, не получится. Минимальное допустимое значение права - **«1»**. Если потребуется игнорировать историю паролей, следует удалить право у пользователя или группы. Эффективным значением является максимальное значение.
SessionDurationLimit	Максимальное время сессии, мин	Устанавливает длительность сессии пользователя. После истечения указанного времени происходит автоматический выход пользователя из системы. Эффективным значением является минимальное значение.
SpecialCount	Количество специальных символов в пароле	Устанавливает минимально допустимое количество специальных символов в пароле. **Специальные символы** ? ! @ # $ % ^ & № < > _ - = + * ( ) [ ] { } . , : ; ~ ` ' " \ | /
UpperCount	Количество в пароле символов в верхнем регистре	Устанавливает минимально допустимое количество символов в верхнем регистре в пароле.
ViewConfiguration	Просмотр конфигурации	Предоставляет доступ к просмотру конфигурации SePlatform.Security без возможности редактирования.
WinKeysShortcutAccess	Доступ к сочетаниям клавиш Windows	Блокирует использование сочетаний клавиш (так называемых Hotkeys). Чтобы запретить использование сочетаний клавиш, укажите их в конфигурационном файле Агент SePlatform.Security. Подробнее об этом в документе на SePlatform.Security, в разделе, описывающем настройку агента.

2. Справочное руководство

2.1. SecurityConfigurator

`SecurityConfigurator` - тип, предназначенный для размещения на форме в проекте SePlatform.HMI.

Тип не является полноценной заменой приложения SePlatform.HMI.SecurityConfigurator: экземпляр типа отличается от приложения тем, что в нем отсутствует верхняя панель инструментов и нижняя строка статуса. Тип следует использовать только для создания собственного приложения SePlatform.HMI.SecurityConfigurator. В остальных случаях используйте одну из форм, предоставляемых расширением.

2.1.1. Свойства

Error

Поле с текстом ошибки приложения. Только для чтения в режиме исполнения. Тип значения - уведомляющий string.

Status

Поле с текстом статуса приложения. Только для чтения в режиме исполнения. Тип значения - уведомляющий string.

CurrentForm

Хранит код статуса открытого во фрейме окна приложения (окно просмотра приложений, окно редактирования пользователя и т.п.). Только для чтения в режиме исполнения. Тип значения - уведомляющий uint1.

pClosed

Ссылка на команду, выполняемую в результате закрытия окна в экземпляре типа.

Настройки (init_Settings)

Ссылка на экземпляр типа 2.2. Настройки (стр. 31), хранящий настройки конфигуратора.

Разрешения (init_Permissions)

Ссылка на экземпляр типа 2.3. Разрешения (стр. 32), хранящий настройки доступа пользователей к файловой системе в диалогах сохранения файлов.

Вызов экранной клавиатуры (init_ScreenKeyboard)

Ссылка на экземпляр типа **`ScreenKeyboardOptions`**, хранящий настройки вызова экранной клавиатуры. Тип предоставляется библиотекой SePlatform.HMI.CommonLib.

2.2. Настройки

Тип предназначен для хранения настроек конфигуратора.

Все экземпляры конфигуратора, сославшиеся на экземпляр этого типа, будут иметь одинаковые настройки.

Настройки описаны в свойствах типа.

2.2.1. Свойства

Пользователь должен быть в группе (UserInAtLeastOneGroup)

Регулирует обязательность добавления пользователя в группу. Тип значения - bool.

> ОБРАТИТЕ ВНИМАНИЕ
>
> Требование обязательного нахождения пользователя в группе теперь исходит из подсистемы безопасности SePlatform.Security.

Значение:

- **«true»** - пользователь должен состоять хотя бы в одной группе. Пока пользователь не будет добавлен в группу, сохранить учетную запись не удастся, так как кнопка сохранения будет неактивна.
- **«false»** - пользователя необязательно добавлять в группу (группы), кнопка сохранения активна. Однако попытка сохранить учетную запись приводит к ошибке.

Пользователь может быть только в одной группе (UserInOnlyOneGroup)

Регулирует количество групп, в которых пользователь может состоять одновременно. Тип значения - bool.

Значение:

- **«true»** - пользователя можно добавить только в одну группу;
- **«false»** - пользователя можно добавить в несколько групп.

Путь к шаблонам приложений (AppTemplatesPath)

Полный путь к папке для хранения шаблонов приложений. Тип значения - string.

Если не указывать значение свойства, то при импорте приложений будет предложен путь к папке по умолчанию. Папкой по умолчанию является папка `Security_Templates` в папке проекта.

Путь к резервным копиям базы (BackupsPath)

Полный путь к папке для хранения резервных копий конфигурации подсистемы безопасности. Тип значения - string.

Если не указывать значение свойства, то при сохранении резервной копии или восстановлении из резервной копии будет предложен путь к папке по умолчанию. Папкой по умолчанию является папка `Backups`, создающаяся в папке проекта при первом сохранении резервной копии.

Папка для экспорта (ExportFolder)

Хранит полный путь к папке, куда пользователь может выполнять экспорт списков пользователей и шаблонов приложений в файлы. Тип значения - string.

По умолчанию списки параметров сохраняются в:

- `C:\ProgramData\SePlatform\HMI.SecurityConfigurator\Export` - для Windows;
- `/home/<user>/SePlatform/HMI.SecurityConfigurator/Export` - для Linux.

Список узлов домена (DomainNodesList)

Список имен АРМ, на которых можно завершить сессию пользователя. Тип значения - string.

Если указать хотя бы одно имя АРМ в сети SePlatform.Net, в окне редактирования учетной записи пользователя появится команда на завершение сессии. Результат применения свойства описан в Специальные команды редактирования учетных записей (стр. 16)).

ПРИМЕР

Построена простейшая сеть SePlatform.Net, в которой все узлы подчинены центральному узлу сети. В сеть включены три АРМ: **`CentralNode`**, **`Node1`** и **`Node2`**. Необходимо иметь возможность завершать пользовательские сессии на узлах **`Node1`** и **`Node2`** из конфигуратора на центральном узле **`CentralNode`**. Тогда в качестве значения свойства DomainNodesList указывается список имен **`Node1`** и **`Node2`**.

2.3. Разрешения

Тип, позволяющий управлять доступом пользователей к файловой системе в диалогах сохранения файлов. Если ограничить доступ, пользователь сможет экспортировать файлы только в папку, указанную в экземпляре типа 2.2. Настройки (стр. 31).

Для определения прав доступа текущего пользователя к файловой системе можно использовать конфигурацию подсистемы безопасности SePlatform.Security. Подробнее - в описании свойств типа.

2.3.1. Свойства

Использовать сервер безопасности для определения прав (UseSecurity)

Позволяет включить использование подсистемы безопасности SePlatform.Security для определения прав доступа текущего пользователя к файловой системе.

Значения:

- **«`true`»** - использовать сервер безопасности для определения прав;
- **«`false`»** - не использовать сервер безопасности для определения прав.

При включении следует заполнить значение свойства Имя приложения с правами безопасности (SecurityApplication).

Доступность файловой системы (FileSystemAccess)

Позволяет включить или отключить доступ пользователя к файловой системе в диалогах сохранения файлов.

Значения:

- **«true»** - файловая система доступна, в диалогах сохранения файлов есть доступ к любой папке;
- **«false»** - файловая система недоступна. Пользователь может сохранять файлы только в папку, указанную в свойстве **Папка для экспорта (ExportFolder)** экземпляра типа 2.2. Настройки (стр. 31).

Имя приложения с правами безопасности (SecurityApplication)

Хранит имя приложения SePlatform.Security, в котором содержится право **FileSystemAccess (Доступность файловой системы)**, регулирующее доступность файловой системы для конкретного пользователя или группы пользователей.

Чтобы использовать сервер безопасности для определения прав текущего пользователя, установите значение **«true»** для свойства **Использовать сервер безопасности для определения прав (UseSecurity)**.

2.4. SecurityConfigurator_App

Экранная форма **SecurityConfigurator_App** - основной компонент SePlatform.HMI.SecurityConfigurator, предназначенный для запуска в виде отдельного приложения. В режиме исполнения является полноценным конфигуратором подсистемы безопасности SePlatform.Security и позволяет:

- создавать, редактировать и удалять учетные записи пользователей;
- создавать, редактировать и удалять группы пользователей;
- добавлять пользователей в группы и удалять их из групп;
- создавать, редактировать и удалять приложения и права, назначать права пользователям и группам;
- создавать роли в приложениях и назначать их пользователям и группам;
- сохранять резервные копии конфигурации и восстанавливать конфигурацию из резервной копии.

Не имеет собственных свойств и функций. Настройки приложения загружаются из конфигурационного файла (стр. 25).

2.5. SecurityConfigurator_Page

Экранная форма **SecurityConfigurator_Page** предназначена для открытия окна конфигуратора во фрейме. В режиме исполнения позволяет:

- создавать, редактировать и удалять учетные записи пользователей;
- создавать, редактировать и удалять группы пользователей;
- добавлять пользователей в группы и удалять их из групп;
- создавать, редактировать и удалять приложения и права, назначать права пользователям и группам;
- создавать роли в приложениях и назначать их пользователям и группам;
- сохранять резервные копии конфигурации и восстанавливать конфигурацию из резервной копии.

Отличается от 2.4. SecurityConfigurator_App (стр. 33) тем, что конфигуратор, открываемой данной формой, можно настроить с помощью свойств.

2.5.1. Свойства

Тема оформления (init_Theme)

Ссылка на экземпляр типа **Theme**, хранящий настройки оформления конфигуратора. Тип предоставляется библиотекой SePlatform.HMI.CommonLib.

Настройки (init_Settings)

Ссылка на экземпляр типа 2.2. Настройки (стр. 31), хранящий настройки конфигуратора.

Разрешения (init_Permissions)

Ссылка на экземпляр типа 2.3. Разрешения (стр. 32), хранящий настройки доступа пользователей к файловой системе в диалогах сохранения файлов.

Вызов экранной клавиатуры (init_ScreenKeyboard)

Ссылка на экземпляр типа **ScreenKeyboardOptions**, хранящий настройки вызова экранной клавиатуры. Тип предоставляется библиотекой SePlatform.HMI.CommonLib.

2.6. SecurityConfigurator_Form

Экранная форма **SecurityConfigurator_Form** предназначена для открытия окна конфигуратора в отдельном окне. В режиме исполнения позволяет:

- создавать, редактировать и удалять учетные записи пользователей;
- создавать, редактировать и удалять группы пользователей;
- добавлять пользователей в группы и удалять их из групп;
- создавать, редактировать и удалять приложения и права, назначать права пользователям и группам;
- создавать роли в приложениях и назначать их пользователям и группам;
- сохранять резервные копии конфигурации и восстанавливать конфигурацию из резервной копии.

Отличается от 2.4. SecurityConfigurator_App (стр. 33) тем, что конфигуратор, открываемой данной формой, можно настроить с помощью свойств.

2.6.1. Свойства

Тема оформления (init_Theme)

Ссылка на экземпляр типа **Theme**, хранящий настройки оформления конфигуратора. Тип предоставляется библиотекой SePlatform.HMI.CommonLib.

Настройки (init_Settings)

Ссылка на экземпляр типа 2.2. Настройки (стр. 31), хранящий настройки конфигуратора.

Разрешения (init_Permissions)

Ссылка на экземпляр типа 2.3. Разрешения (стр. 32), хранящий настройки доступа пользователей к файловой системе в диалогах сохранения файлов.

Восстанавливать положение окна (init_RestoreWindow)

Позволяет восстанавливать положение окна после его повторного открытия. Тип значения - bool

Значения:

- **«true»** - положение окна запоминается. Окно откроется в том же месте, где было закрыто.
- **«false»** - положение окна не запоминается. Окно откроется в координатах по умолчанию.

Вызов экранной клавиатуры (init_ScreenKeyboard)

Ссылка на экземпляр типа **ScreenKeyboardOptions**, хранящий настройки вызова экранной клавиатуры. Тип предоставляется библиотекой SePlatform.HMI.CommonLib.

2.7. SecurityConfigurator_Tests

Форма предназначена для ознакомления с примерами использования форм расширения 2.6. SecurityConfigurator_Form (стр. 34) и 2.5. SecurityConfigurator_Page (стр. 33) в проекте SePlatform.HMI.

Чтобы ознакомиться с этими примерами, откройте форму в режиме редактирования. Ознакомьтесь с обработчиками событий MouseClick кнопок **Отдельным окном** и **Во фрейме**.

История изменений

2.2

Новая возможность

Разработана возможность ограничения доступа пользователей к файловой системе.

- Создан тип 2.3. Разрешения (стр. 32) (SecurityConfigurator_Permissions) со свойством **FileSystemAccess (Доступность файловой системы)**, значение которого регулирует доступ к системе.
- Типу 2.2. Настройки (стр. 31) (SecurityConfigurator_Settings) добавлено свойство **ExportFolder (Папка для экспорта)**.

Если у пользователя отсутствует доступ к файловой системе (FileSystemAccess = false), то в файловых диалогах будет недоступен просмотр дерева папок и создание новых папок, а экспорт будет возможен только в папку экспорта, указанную в свойстве **ExportFolder**. По умолчанию папкой для экспорта является:

- `C:\ProgramData\SePlatform\HMI.SecurityConfigurator\Export` - в ОС Windows.
- `/home/<user>/SePlatform/HMI.SecurityConfigurator/Export` - в ОС Linux.

Улучшения

- Пункты контекстного меню с командами на изменение конфигурации скрыты, если пользователю запрещено редактирование конфигурации.
- Теперь при назначении прав пользователю или группе в окне выбора прав не отображаются уже назначенные права.
- При создании новой роли все права приложения больше не назначаются ей автоматически. Права приложения можно добавить или удалить, как это делается для групп и пользователей.

Изменение

Исключена возможность экспорта информации в файлы `*.pdf` во всех местах, где можно выполнить экспорт:

- экспорт списка пользователей и их прав;
- экспорт таблицы "Список прав и их значений для приложения" со страницы списка приложений;
- экспорт прав открытого на редактирование приложения.

Исправления

- Исправлена ошибка, из-за которой пользователю, добавленному в группу с нулевым значением права "История паролей", нельзя было установить текущий пароль.
- Теперь при авторизации пользователя после изменения парольных политик предлагается сменить пароль, если старый пароль не подходит новым парольным политикам. Ранее в таком случае возникала ошибка.
- Устранена причина, по которой после импорта приложения в таблице прав роли отображались не сразу, а, например, только после перехода к редактированию приложения.
- При изменении размеров окна выбора прав кнопки "Добавить" и "Отмена" оставались на месте, из-за чего ими было неудобно пользоваться. Теперь кнопки перемещаются соответственно изменению размеров окна.

2.2.1

Улучшения

- Тип **Разрешения (SecurityConfigurator_Permissions)** теперь позволяет использовать сервер безопасности для определения прав доступа пользователя к файловой системе.
- Панель инструментов теперь оформляется в соответствии с выбранной темой.

Исправление

При использовании SePlatform.HMI.WebViewer разделитель областей окна конфигуратора не позволял нормально изменять их размеры.

Изменения документации

Редакция 1

В руководстве пользователя:

- В разделе 1.4.8. Безопасность в компонентах Систэм Платформ (стр. 22) актуализирован список шаблонов приложений SePlatform.Security, поставляемых с дистрибутивом конфигуратора.
- Исключено упоминание возможности экспорта данных в файлы `*.pdf`.
- Обновлены скриншоты.

В справочном руководстве описаны новые компоненты 2.2. Настройки (стр. 31) и 2.3. Разрешения (стр. 32), а также их свойства. Для компонентов 2.1. SecurityConfigurator (стр. 30), 2.6. SecurityConfigurator_Form (стр. 34) и 2.5. SecurityConfigurator_Page (стр. 33) описаны новые свойства - ссылки на экземпляры типов 2.2. Настройки (стр. 31) и 2.3. Разрешения (стр. 32).

2.1

Новые возможности

- Внешний модуль **SecurityConfigurator** предоставляет новые компоненты для разработки проектов SePlatform.HMI:
  - тип **SecurityConfigurator**, предназначенный для размещения на форме;
  - форма **SecurityConfigurator_Page** - аналог прежней формы **SecurityConfigurator**, предназначенный для открытия во фрейме;
  - форма **SecurityConfigurator_Form** - аналог прежней формы **SecurityConfigurator**, предназначенный для открытия в виде отдельного окна;
  - форма **SecurityConfigurator_App** - основная форма, предназначенная для запуска в виде отдельного приложения;
  - тип **SecurityConfigurator_Settings**, предназначенный для упрощения настройки экземпляров конфигуратора, создаваемых на основе указанных выше типов и форм.
- Для типа **SecurityConfigurator** и форм **SecurityConfigurator_Page**, **SecurityConfigurator_Form** можно:
  - выбрать тему оформления.
  - настроить вызов экранной клавиатуры в файловых диалогах.
- Реализована возможность экспорта и импорта собственных шаблонов приложений.

Улучшения

- Настройки самостоятельного приложения SePlatform.HMI.SecurityConfigurator теперь сохраняются в конфигурационный файл `app_settings.json`, расположенный в:
  - `C:\ProgramData\SePlatform\HMI.SecurityConfigurator` (ОС Windows);
  - `/home/<user>/SePlatform/HMI.SecurityConfigurator` (ОС Linux).
- Перед удалением учетной записи пользователя теперь проверяется его активность на удаленных рабочих станциях, указанных в настройках экземпляра конфигуратора.
- Всплывающая подсказка с текстом ошибки теперь отображается всегда, без необходимости наведения мыши на элемент с ошибкой:
  - в окне редактирования учетной записи пользователя;
  - в окне смены пароля учетной записи пользователя.
- В окне просмотра учетных записей теперь можно создавать, редактировать и удалять учетные записи с помощью клавиатуры или контекстного меню. Аналогично в окне просмотра приложений можно создавать, редактировать и удалять приложения с помощью клавиатуры или контекстного меню.
- В окне просмотра групп вызвать контекстное меню для создания новой группы теперь можно без выделения существующей группы.
- Добавлены шаблоны приложений безопасности для решений SePlatform.HMI.SetPoints и SePlatform.HMI.IntegrityControl.
- Обновлен шаблон приложения безопасности для SePlatform.HMI.Trends.
- В интерфейсе конфигуратора обновлены иконки.

2.1.1

Исправления

- Исправлены ошибки, возникавшие при создании новых учетных записей:
  - Не удавалось сохранить новую учетную запись, если при ее создании поле **Пароль** заполнялось в последнюю очередь.
  - Не появлялась всплывающая подсказка о несовпадении значений из полей **Пароль** и **Подтверждение**.
- Устранена причина повторного входа в подсистему безопасности при использовании клавиши **Enter** в окне авторизации пользователя.

2.1.2

Новая возможность

Теперь при экспорте списка пользователей в файл можно дополнительно создать файлы с перечнем эффективных прав каждого пользователя.

Исправление

Устранена причина, по которой использование клавиши Enter после ввода названия новой группы приводило к ошибке.

Изменения документации

Редакция 2

В руководстве пользователя:

- Актуализирован раздел 1.3. Запуск приложения (стр. 7).
- Раздел **Хранение конфигурационных файлов** переименован в 1.5. Настройка приложения в конфигурационных файлах (стр. 25) и расширен.
- Раздел **Безопасность в приложениях** переименован в 1.4.8. Безопасность в компонентах Систэм Платформ (стр. 22) и актуализирован.
- Обновлены скриншоты.

Актуализировано справочное руководство.

Редакция 3

В руководстве пользователя:

- В разделе 1.4.3. Создание приложений и прав (стр. 12) создан подраздел, описывающий экспорт и импорт приложений (стр. 13).
- В разделе 1.4.6. Создание и редактирование учетных записей пользователей (стр. 16) создан подраздел, описывающий экспорт списка пользователей и списков их эффективных прав (стр. 20).
- Имя администратора SePlatform.Security по умолчанию изменено с **«AdminQA»** на **«administrator»**. Имя администратора было обновлено в SePlatform.Security 1.4.9.
- Обновлены скриншоты.

В истории изменений исправлен ошибочно указанный номер предыдущей редакции. Вместо "Редакция 1" указано "Редакция 2".

2.0

Важно. Текущая версия предназначена для использования с SePlatform.HMI 2.0.

Изменения документации

Редакция 1

Внутренние изменения. Содержимое документа не изменилось.

1.2

Новая возможность

Списки приложений и пользователей теперь можно экспортировать в файлы форматов `*.csv`, `*.xlsx`, `*.pdf`.

Примечание: свойство **Путь для экспорта таблиц** формы **SecurityConfigurator**, разрабатывавшееся для реализации этой возможности, удалено из интерфейса, так как более неактуально.

Улучшения

- В окне просмотра списка приложений появилась таблица предварительного просмотра приложений. Теперь при выборе приложения из списка в области справа отображается информация о правах приложения, их значениях и назначениях.
- В окне просмотра списка пользователей теперь отображается больше информации о пользователях. Помимо логина и отображаемого имени в таблице появились номера телефонов, должности, роли и пр. Набор столбцов таблицы можно менять.

Изменения документации

Редакция 1

В руководстве пользователя описано, как экспортировать списки приложений (стр. 13) и пользователей (стр. 20) в файлы форматов `*.csv`, `*.xlsx`, `*.pdf`.

Из справочного руководства удалено упоминание устаревшего свойства **Путь для экспорта таблиц** формы **`SecurityConfigurator`**.

Во всем документе актуализированы скриншоты.

Редакция 2

Информация о конфигурационных файлах приложения актуализирована и перенесена из подраздела 1.3. Запуск приложения (стр. 7) -> "Настройки вида приложения" в новый раздел - 1.5. Настройка приложения в конфигурационных файлах (стр. 25).

1.1

1.1.1

Улучшение

В наборе компонентов, предоставляемых внешним модулем **`SecurityConfigurator`**, появилась новая экранная форма - **`SecurityConfigurator_Tests`**. Форма предназначена для ознакомления с примером встраивания конфигуратора безопасности в проект SePlatform.HMI - здесь окно конфигуратора открывается по нажатию на кнопку **`Настройка пользователей`**.

Исправления

- Иконка права **`PasswordAge (Срок действия пароля, дней)`** в окне выбора прав отображалась некорректно при использовании приложения на ОС Linux.
- Устранена причина, по которой в окне редактирования учетных записей не сохранялась установленная вручную ширина столбцов.

Изменения документации

Редакция 2

Внутренние изменения. Содержимое документа не изменилось.

Редакция 3

В руководстве пользователя:

- В разделе 1.3. Запуск приложения (стр. 7) описано назначение новой экранной формы расширения - **`SecurityConfigurator_Tests`**.
- Обновлен раздел 1.4.7. Получение эффективных значений прав (стр. 21). Пример, приведенный в разделе, описан короче и проще.
- Актуализированы скриншоты.